

Security, Data Protection, and Architecture

Architecture, access control, encryption, AI processing, and data handling for the hosted Pathway platform.

VERSION

1.0

DATE

October 2026

SCOPE

Hosted platform

CONTACT

hi+support@lendpathway.com

COMPANY

Pathway Systems LLC

WEBSITE

lendpathway.com

TERMS

lendpathway.com/terms

PRIVACY

lendpathway.com/privacy

Contents

01	Summary	2
02	Platform overview	3
03	Architecture	5
04	Data flows and trust boundaries	7
05	Data inventory	9
06	Customer identity and access	10
07	Authorization and tenant isolation	12
08	Encryption and secret management	13
09	AI processing and the chat agent	14
10	Application and infrastructure security	15
11	Logging, monitoring, and audit records	16
12	Data retention, deletion, and export	17
13	Availability, backup, and business continuity	18
14	Incident response and vulnerability management	19
15	Personnel and internal access	19
16	Subprocessors and connected services	20
17	Privacy and compliance	22
18	Shared responsibility	23
19	Answers to common questionnaire items	24
20	Contact	25

About this document

This document describes the security controls of the hosted Pathway platform. It is written for security, compliance, and procurement reviewers. Each section answers one group of questions that reviewers usually ask. Section 19 gives short answers to common questionnaire items. Section 16 lists the subprocessors.

The document describes the platform as deployed on the date on the cover. It is provided for information and does not create contractual obligations.

Applies to	The hosted, multi-tenant Pathway platform at <code>app.lendpathway.com</code> and its API.
Does not apply to	Self-hosted deployments. These are covered by a separate agreement and a separate deployment guide.
Related documents	lendpathway.com/terms and lendpathway.com/privacy . Where this document and a signed agreement differ, the signed agreement controls.
Terminology	Customer Data means all documents, parsed outputs, structured data, and derived analytics that a customer uploads to or generates within its organization on the platform. Organization means one customer tenant. Book means the set of documents and data for one deal.

01 Summary

Pathway is a hosted underwriting workspace for lenders and brokers. Customers upload or forward merchant documents such as bank statements, tax returns, credit reports, and applications. Pathway extracts the financial data in those documents, verifies it against the totals printed on the documents, and presents it for review, screening, and downstream actions.

Pathway processes sensitive financial information about small businesses and their owners. The platform is designed around four principles:

- **One tenant, one boundary.** Every record belongs to one organization. The API applies the organization of the caller to every query. There is no cross-tenant read path.
- **Managed infrastructure, few moving parts.** Pathway runs on established managed providers in the United States. Pathway does not operate its own servers, networks, or data centers.
- **Customer Data is used only to provide the service.** Pathway does not sell Customer Data, does not use it for advertising, and does not use it to train AI models. AI providers process data under API terms that exclude training.
- **The customer stays in control.** Customers own their data, can export it in full, can delete it, and control every connection to an external service.

Control summary

AREA	CONTROL	STATUS
Encryption in transit	TLS 1.2 or later on every connection. HTTP Strict Transport Security with preload on the web application.	In place
Encryption at rest	Provider-managed encryption for object storage, the database, and the cache. Selected credentials are also encrypted at the application layer.	In place
Authentication	Auth0 Universal Login. Sign-in with Google, Microsoft Entra ID, or email and password with a verified code. Multi-factor authentication is available.	In place

AREA	CONTROL	STATUS
Authorization	Three organization roles. Organization-scoped queries. A fail-closed write guard for read-only principals.	In place
Tenant isolation	Application-layer isolation per organization. Per-tenant object key prefixes. Separate production and staging environments.	In place
AI data use	Provider APIs under terms that exclude model training. Requests to OpenAI are marked for no storage.	In place
Data deletion	Users delete documents, Books, chats, tokens, and connections in the application. Removal of all Customer Data on written request.	In place
Data export	Spreadsheet, CSV, and PDF exports in the application. Full export of Customer Data on request.	In place
Backups	Automated database backups with point-in-time recovery. Object storage designed for 99.999999999% durability.	In place
Incident notification	Affected customers are notified by email after a confirmed incident.	In place
Production access	Three named individuals. One designated administrator for production configuration changes. MFA on every provider account.	In place
Independent audit	Pathway does not hold a SOC 2 report at this time. Infrastructure and identity providers hold their own SOC 2 Type II reports.	Disclosed

02 Platform overview

What the platform does

A customer creates an organization. Members of the organization create Books. A Book holds the documents for one deal. Pathway parses those documents into structured data: the business, its bank accounts, every transaction, tags, debt positions, and the content of credit reports, tax forms, and applications. Users review the result, correct tags, exclude documents, and run screening rules. Users can then export spreadsheets, fill contracts, match the deal to funding partners, send emails, or push data to a connected system.

All derived views are computed from the parsed data at read time. Pathway stores the source documents and the parsed data. It does not store a separate copy of every report.

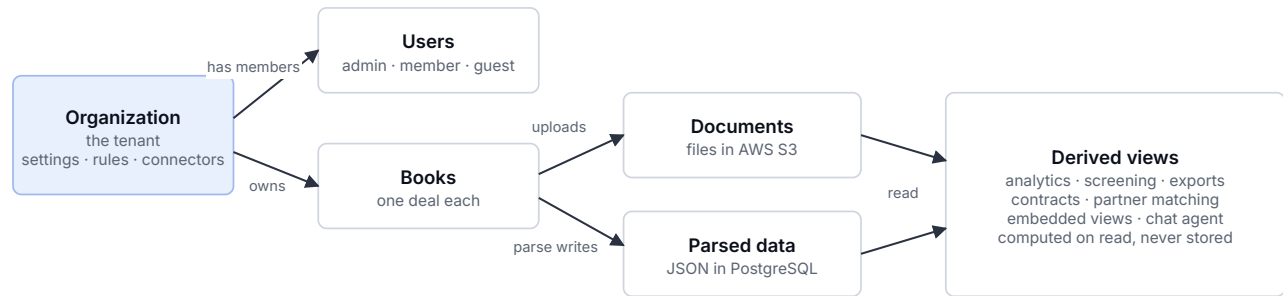


Figure 1. The data model. Every object belongs to one organization. Derived views are computed on read.

Product surfaces

SURFACE	DESCRIPTION	CREDENTIAL
Web application	The main workspace in a browser. Books, documents, analytics, screening, settings, integrations, and chat.	Auth0 session (JWT)
API	Programmatic submission of documents, parse status, webhooks, and read access to parsed data.	Personal access token
Embedded views	A read-only view of one Book that a customer can place in its own system or share with a counterparty.	Embed token, one Book
Email intake	Deal submissions sent to an organization-specific address or read from a connected inbox become Books automatically.	Mailbox grant
Chat agent	An assistant that can read Books and run code in an isolated sandbox with the user's permissions.	Auth0 session plus a read-only token for the sandbox

Deployment options

OPTION	DESCRIPTION
Hosted platform	Multi-tenant service operated by Pathway in the United States. This document describes this option.
Self-hosted	The platform runs in the customer's own infrastructure with the customer's own provider keys. Available under a separate agreement, with optional source code escrow.

03 Architecture

Pathway runs on managed providers. The web application is static and is served from a content delivery network. The API, the database, and the cache run in one hosting project on a private network. Documents are stored in a private object storage bucket. Identity is delegated to Auth0. AI and verification providers are called from the API only. AI and verification providers are called from the API only.

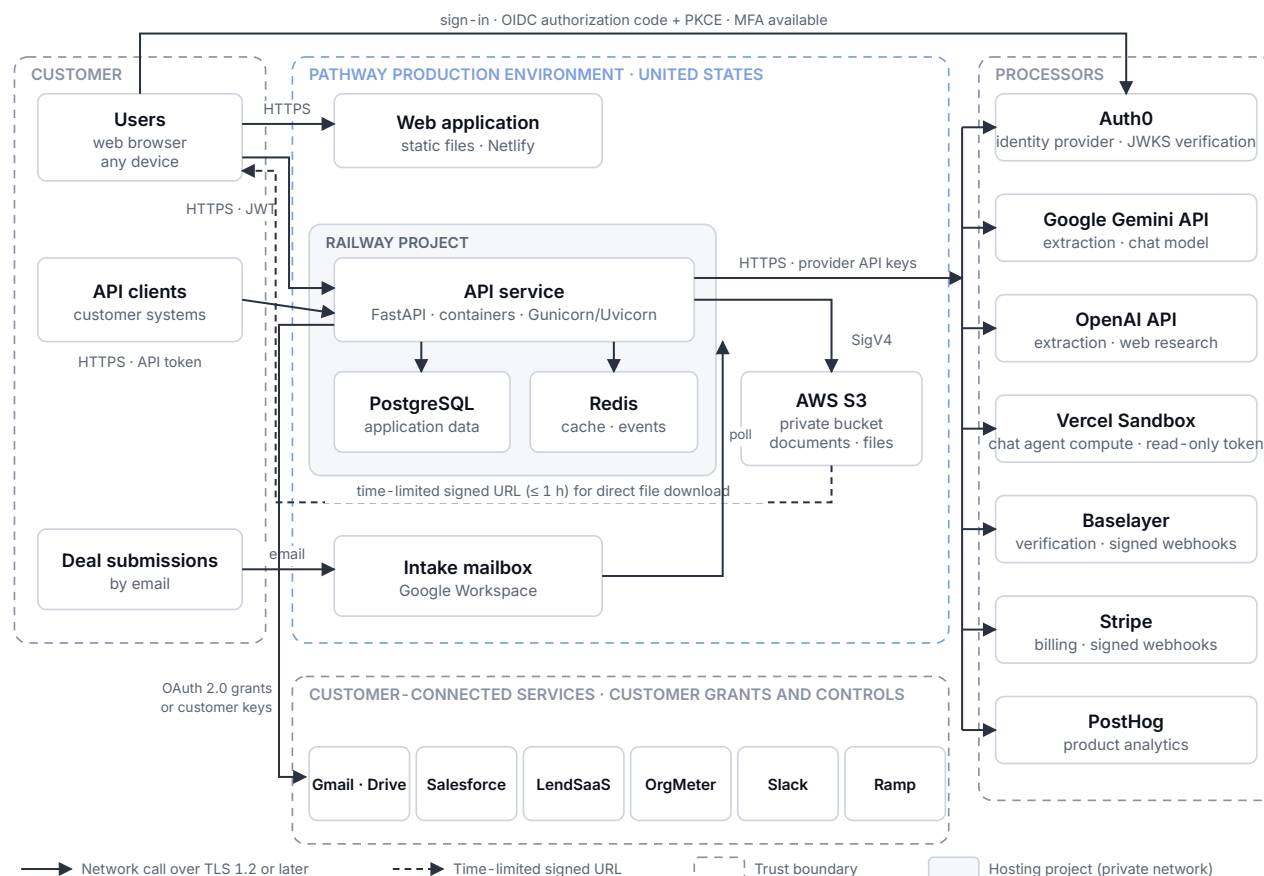


Figure 2. Production architecture and trust boundaries. Every arrow is an HTTPS connection unless marked otherwise. Browsers download documents directly from object storage with signed URLs that expire within one hour.

Reading the diagram

- **One path to data.** The API service is the only component that reads or writes the database, the cache, and object storage. The web application is static and holds no Customer Data.
- **Private data stores.** The database and the cache are reachable only inside the hosting project. The object storage bucket is private and is accessed with signed requests.
- **Identity is delegated.** Users sign in at Auth0. The API verifies each token against Auth0's published keys and never handles passwords.
- **Processors are called, never calling.** AI, verification, and billing providers receive requests from the API with Pathway's keys. The only inbound traffic from them is signed webhooks.

Components

COMPONENT	TECHNOLOGY	OPERATED BY	ROLE
Web application	React single - page application, static files	Netlify	User interface. Holds no Customer Data at rest. Served with HSTS.
API service	Python, FastAPI, Gunicorn and Uvicorn workers in a container	Railway	All business logic, authorization, parsing, and integrations. The only component that reads the database, the cache, and object storage.
Database	PostgreSQL 18, managed	Railway	Organizations, users, Books, parsed data, settings, tokens, usage ledger.
Cache and events	Redis 7, managed	Railway	Short-lived caches, event streams, locks, and in-flight OAuth connection attempts.
Object storage	Amazon S3, private bucket, server-side encryption	AWS	Uploaded documents, generated exports, chat uploads, and chat artifacts.
Identity provider	Auth0 with the custom domain <code>auth.lendpathway.com</code>	Auth0 (Okta)	Sign-in, password storage, verification codes, token issuance.
Intake mailbox	Google Workspace mailbox, Gmail API	Google	Receives deal submissions by email and sends replies and invitations.
AI providers	Google Gemini API, OpenAI API	Google, OpenAI	Document extraction, classification, web research, and the chat model.
Chat sandbox	Vercel Sandbox, isolated Linux micro-VM	Vercel	Short-lived compute for the chat agent. Created per chat, stopped automatically.
Verification	Baselayer API	Baselayer	Business verification and public records, on user request.
Billing	Stripe Checkout, Billing Portal, webhooks	Stripe	Subscriptions and payments. Payment details never reach Pathway.
DNS	Cloudflare DNS	Cloudflare	Name resolution for Pathway domains. No Customer Data.

Environments

Production and staging are separate hosting projects. Each has its own database, cache, object storage bucket, secrets, and provider keys. Local development runs against local containers, not production data.

Network model

- The web application and the API are reachable only over HTTPS. The web application sends HTTP Strict Transport Security headers with preload.
- The API accepts browser requests only from the allow-listed application origins. Other origins are refused by the CORS policy.
- The database and the cache are reachable from the API over the hosting project's private network. They are not exposed to the public internet.
- The object storage bucket is private. The API signs each request. Browsers receive signed URLs that expire within one hour, or within five minutes for chat files.
- Inbound webhooks from Stripe and Baselayer are verified with a signing secret before they are processed.
- Outbound requests to addresses supplied by users (for example, a document link in an email) are refused if they resolve to a private, loopback, or link-local address.

04 Data flows and trust boundaries

The table lists each path that Customer Data or credentials can take. "Protection" names the control on that path. Every path uses TLS 1.2 or later.

#	PATH	DATA	PROTECTION
1	Browser → Web application	Static application files only.	HTTPS, HSTS preload. No Customer Data is served from this path.
2	Browser → Auth0	Sign-in credentials, verification codes, profile claims.	OpenID Connect authorization code flow with PKCE. Pathway never receives passwords.
3	Browser → API	All application requests and uploads.	Bearer JWT verified against Auth0's signing keys. CORS allow-list. Upload size limit of 100 MB per file.
4	API client → API	Document submissions, status reads, data reads.	Personal access token, stored as a SHA-256 hash. Per-token rate limit. Optional read-only scope.
5	API → Database, Cache	All application records.	Private network inside the hosting project. Credentials held as platform secrets.
6	API → Object storage	Document bytes, exports, chat files.	Signed requests (AWS Signature Version 4). Private bucket. Random object names under a per-tenant and per-Book prefix.

#	PATH	DATA	PROTECTION
7	Object storage → Browser	One document at a time.	Signed URL with an expiry of one hour or less. The URL names the object only. The bucket is otherwise closed.
8	API → AI providers	Document pages or text, extracted transactions, business names for research.	Provider API over HTTPS. API terms that exclude training. No storage flag on OpenAI requests. Organization identifier sent as a hash.
9	API ↔ Chat sandbox	Book data and files the user attached to the chat. A read-only API token for that chat.	Isolated micro-VM per chat. Token is read-only and revoked when the chat is deleted. Sandbox stops automatically.
10	API ↔ Baselayer	Business name, address, tax identifier, owner names, when a user runs a verification.	API key held as a platform secret. Inbound webhooks verified by signature.
11	API ↔ Stripe	Billing contact, subscription state.	Hosted checkout and portal. Card data never reaches Pathway. Webhooks verified by signature.
12	Email sender → Intake mailbox → API	Message headers, attachments, and links to documents.	Organization-specific address. Sender allow-lists. Attachments stored to object storage. Message bodies are not retained beyond processing.
13	API ↔ Customer-connected services	Only what the customer's workflow sends or reads: emails, Drive files, CRM records, Slack messages.	OAuth 2.0 grants or customer-supplied keys. Granted by the customer, revocable at any time. Grants are deleted on disconnect.
14	API → Product analytics	Event names, user and organization identifiers, pages viewed.	No document content, parsed data, or message content is sent.

Trust boundaries

Three boundaries matter. The customer boundary: browsers, API clients, and email senders. The Pathway production boundary: the web application, the API, the database, the cache, the intake mailbox, and object storage. The processor boundary: providers that process data under Pathway's contracts. Customer-connected services sit outside all three. The customer grants and revokes them.

05 Data inventory

This table lists the categories of data that Pathway stores, where each is stored, how it is protected, and how long it is kept.

CATEGORY	EXAMPLES	STORAGE	PROTECTION	RETENTION
Customer documents	Bank statements, tax returns, credit reports, applications, identity documents, voided checks, exports.	Amazon S3, production bucket	Private bucket. Server-side encryption. Per-tenant key prefix. Random object names. Signed URLs ≤ 1 hour.	Life of the account. Removed on written request.
Parsed financial data	Business and owner names, account numbers as printed, transactions, balances, tags, debt positions, credit and tax fields, user edits.	PostgreSQL	Provider encryption at rest. Every read and write is scoped to the organization.	Same as documents.
Account and identity data	Name, verified email, verified phone, profile picture, login provider, organization memberships, roles.	PostgreSQL and Auth0	Only identifiers that the identity provider verified are stored. Passwords are held by Auth0 only.	Until the user or organization is deleted.
Connector credentials	OAuth tokens for Gmail, Drive, and Salesforce. Customer API keys for LendSaaS and OrgMeter. Slack destinations. Ramp merchant tokens.	PostgreSQL	Provider encryption at rest. Never sent to a browser. Selected tokens are also encrypted with an application key held outside the database.	Deleted when the customer disconnects the service.
API and embed tokens	Personal access tokens, embed tokens, invitation tokens.	PostgreSQL and Redis	Access tokens stored as SHA - 256 hashes; only a prefix is displayed. Embed and invitation tokens are random and time-limited.	Until revoked or expired.

CATEGORY	EXAMPLES	STORAGE	PROTECTION	RETENTION
Usage and billing records	One ledger row per parse, chat turn, research call, or verification; subscription state; invoices (at Stripe).	PostgreSQL and Stripe	Written in the same transaction as the work. Not editable through the application.	Life of the account, then as required for financial records.
Email intake records	Sender, forwarder, subject, message identifiers, attachment list, processing status.	PostgreSQL	Organization-scoped. Message bodies are read for attachments and links and are not stored.	Life of the account.
Chat history	Messages, tool calls, tool results, attachments, saved artifacts.	PostgreSQL and Amazon S3	Owned by the user who created the chat. Scoped to that organization.	Until the chat is deleted.
Product analytics	Event names such as "parse started", user and organization identifiers, pages viewed.	PostHog (United States)	No document content, parsed values, or message content.	Per the provider's retention setting.
Application logs	Request method, path, status, duration; application events and errors.	Hosting provider log stream	Tokens in paths are redacted. Document content is not logged.	Short-term, per the provider's retention.

Data classification

Pathway treats all Customer Data as confidential. Customer documents and parsed financial data are the most sensitive category. They can contain personal information about business owners, including names, addresses, account numbers, and tax identifiers. Connector credentials and tokens are secrets. Account data is personal data of the customer's users. Usage records, intake records, and logs are operational data.

06 Customer identity and access

Sign-in

Pathway delegates authentication to Auth0. Users sign in on the hosted login page at `auth.lendpathway.com`. Pathway has no login form of its own and never receives a password.

METHOD	DESCRIPTION
Google	OpenID Connect through Google. Email is verified by Google.
Microsoft Entra ID	OpenID Connect through the Microsoft identity platform. The customer's conditional access and MFA policies apply. Email is verified by a code on first sign-in.
Email and password	Managed by Auth0. A verification code is required before the account is created. Passwords are stored by Auth0 as salted hashes. Password reset uses a code sent to the verified email.
Multi-factor authentication	Available through Auth0. Customers who sign in through Google or Microsoft Entra ID enforce MFA in their own identity provider.

Sessions and tokens

- The web application uses the OpenID Connect authorization code flow with PKCE.
- The API accepts an access token signed with RS256. The API verifies the signature against Auth0's published keys, and checks the audience, the issuer, and the expiry on every request.
- Access tokens expire after 24 hours. Refresh tokens rotate on each use, expire after 30 days, and expire after 15 days without use. Reuse of a rotated refresh token is refused.
- Sign-out ends the session in the browser and at Auth0.
- Pathway stores only identifiers that the identity provider has verified. A sign-in with neither a verified email nor a verified phone is refused.

Organization roles

ROLE	PERMISSIONS
Admin	Everything a member can do. Also: invite and remove members, change roles, change organization settings and screening rules, connect and disconnect organization-level services, manage billing.
Member	Create and edit Books, upload and delete documents, run parses, edit tags and positions, run exports and actions, connect personal services such as Gmail and Drive.
Guest	Read-only. Every request that would change data is refused by the API's write guard, whatever the endpoint.

Invitations

An admin invites a member by email. The invitation is a random token bound to the organization, the email address, and the role. It expires after 7 days and can be used once. Acceptance requires a sign-in whose verified email matches the invited address. An admin can revoke a pending invitation. Removing a member removes their access to the organization at once.

Personal access tokens

- A token is bound to one user and one organization. It carries that user's role.

- The raw value is shown once at creation. Pathway stores a SHA-256 hash and a short prefix for display.
- A token can be created as read-only. A read-only token cannot change data. Tokens can be revoked at any time and are rate-limited per token.

Embed tokens

An embed token grants read-only access to one Book and nothing else. The API checks that every request made with it stays within that Book. Tokens are random, expire after 24 hours by default, cannot change data, and cannot create other tokens.

07 Authorization and tenant isolation

Pathway is a multi-tenant platform with isolation at the application layer. Every row in the database and every object in storage belongs to exactly one organization. The API resolves the caller's identity and organization before it runs any query, and it includes that organization in the query.

How a request is authorized

- 01 The API identifies the credential: an embed token, a personal access token, or a session JWT. Each is validated as described in Section 6.
- 02 The API resolves the acting organization. A session may name an organization in a header; membership in that organization is checked. A personal access token is bound to one organization, and a conflicting header is refused. An embed token is bound to one Book.
- 03 For a request that changes data, a middleware checks that the principal can write. Guests, embed tokens, and read-only tokens are refused. If the check cannot complete, the request is refused.
- 04 The endpoint applies its own checks: the organization filter on every query, the single-Book scope for embed tokens, and admin-only checks for membership, settings, and integration changes.
- 05 Organization-level routes that name an organization in the path refuse any organization other than the acting one.

Isolation controls

LAYER	CONTROL
Database	Every table that holds Customer Data has an organization column. Every query includes it. Lists are paged and filtered in SQL, not in the browser.
Object storage	Object keys are prefixed by tenant and Book. Object names are random. No listing operation is exposed to users. A signed URL names one object and expires.
Cache	Keys carry the identity they belong to. Cached identity lookups expire within one hour. User deletion clears its entries at once.

LAYER	CONTROL
Background work	Parses, intake polling, and connector synchronization run in the same service under the organization they were started for. A background write is accepted only while the job that started it is still the current job for that Book.
Chat agent	The agent acts with a read-only token bound to the user and organization. Writes return an error. The token is revoked when the chat is deleted.
Internal administration	Cross-organization administration is a separate set of routes, available only to a session whose user holds the internal administrator flag. Read-only principals cannot reach those routes even when the underlying user is an administrator.

Verification

Pathway maintains automated tests that run against a live API and database. The tests create a disposable organization with users of each role. They check that guests, read-only tokens, and embed tokens cannot change data, that an embed token cannot read another Book, and that members cannot perform admin actions.

08 Encryption and secret management

In transit

- Every connection to the web application, the API, the identity provider, and object storage uses TLS 1.2 or later. Certificates are issued and renewed by the hosting providers.
- The web application and the public website send Strict-Transport-Security with a one-year maximum age, includeSubDomains, and preload.
- Calls from the API to every provider use HTTPS. Calls from the API to the database and the cache stay inside the hosting project's private network.

At rest

- Object storage uses server-side encryption managed by AWS. The bucket is private.
- The database and the cache run on encrypted volumes managed by the hosting provider.
- Selected third-party credentials, such as merchant tokens issued by a partner program, are additionally encrypted at the application layer with a key held outside the database.
- Personal access tokens are stored as SHA-256 hashes. Passwords are stored by Auth0 as salted hashes and never reach Pathway.

Secrets

- Provider keys, database credentials, signing secrets, and encryption keys are stored as environment secrets in the hosting platform. They are not in source control. Configuration files that hold secrets are excluded from the repository.
- Production and staging have separate secrets. A staging key cannot reach production data.

- Each external provider has its own key. A key grants only the access that the integration needs.
- Secrets are rotated when a person with access leaves, when a provider advises rotation, or when exposure is suspected.
- Inbound webhooks are accepted only with a valid signature from the provider's signing secret.

Keys for customer -connected services

OAuth grants that users give to Pathway, such as Gmail or Google Drive access, are stored server-side only. They are never sent to a browser or to the chat sandbox. When the user disconnects the service in Pathway, the grant and its tokens are deleted. Users can also revoke the grant from their Google or Microsoft account settings. Either action stops access at once.

09 AI processing and the chat agent

Pathway uses large language models to read documents and to power the chat agent. All model calls are made from the API with Pathway's provider keys. No model is trained on Customer Data.

What is sent to AI providers

TASK	PROVIDER	DATA SENT	RETURNED
Document extraction	Google Gemini API, or OpenAI API when the organization selects it	Document pages or extracted text, and the structure that the output must follow.	Structured JSON: accounts, transactions, fields.
Classification and reconciliation	Same as extraction	Normalized transaction descriptions, the organization's funder directory, discrepancies to resolve.	Tags, positions, corrections.
Web research	OpenAI API	The business name and location, to look up public information.	A text summary with sources.
Chat agent	Google Gemini API	The conversation, the Books and files the user attached, and tool results.	Text, tool calls, and artifacts.
Image generation	fal.ai	The user's text prompt only.	An image.

Provider terms and controls

- Pathway uses the providers' API services under their business terms. Under those terms the providers do not use API inputs or outputs to train their models.
- Requests to OpenAI are sent with storage disabled, so the request is not kept in the provider's conversation storage.

- Each request carries a hashed organization identifier so that the provider's abuse controls can be applied per tenant without disclosing the tenant.
- Every model call validates the response against a fixed schema. A response that does not match the schema is rejected. The model cannot write free text into a financial field.
- Every model call is recorded in the usage ledger with the organization, the Book, the job, the model, and the token counts. No prompt content is stored. Extracted bank data is checked against the totals printed on each statement, and a ledger that does not reconcile is flagged in the user interface.

The chat agent and its sandbox

The chat agent can run code. It does so in a disposable Linux sandbox from Vercel, not in Pathway's API service. The sandbox is created for one chat, stops automatically after 45 minutes of inactivity, and discards its files when it stops. Only outputs that the agent saves explicitly are kept, in object storage under a random key.

CONTROL	DESCRIPTION
Permissions follow the user	The sandbox receives a personal access token for the chat's owner, marked read-only and bound to the organization. The agent cannot change data through the API.
Credentials stay server-side	Gmail, Salesforce, and Slack credentials never enter the sandbox. Those tools run inside the API with the user's existing grants. Inbox reads go through a read-only proxy.
Sending requires approval	An email composed by the agent is shown to the user and is sent only after the user approves it.
Tools are opt-in per chat	Each chat enables only the connectors the user turns on. The agent receives no tool it was not given.
Bounded runs	Each turn has a time limit and a limit on tool rounds. The user can stop a run at any time.
Revocation	Deleting a chat revokes its token, stops its sandbox, and removes its history.

10 **Application and infrastructure security**

Secure development

- All source code is held in a private version-controlled repository.
- Dependencies are pinned to exact versions. The container image is rebuilt from the pinned list on every deploy.
- Database migrations run as a pre-deploy step. A migration that fails stops the deploy. The previous version keeps serving.
- Deploys overlap: the previous version keeps serving until the new version is healthy. The service shuts down gracefully and records any work that was interrupted.
- Parser output is regression-tested twice a day against published baselines.

- Authorization behavior is covered by automated tests that run against a live API and database (Section 7).

Input handling

- Uploads are limited to 100 MB per file. The file type is detected from the content, not from the file name. Only recognized document types are parsed.
- Email attachments and ZIP archives are expanded with size checks before any file is stored.
- Links in emails are followed only to public addresses. Requests to private, loopback, or link-local addresses are refused, including after redirects.
- Every request body is validated against a typed schema. Invalid requests are refused with a validation error and are not processed.
- Email content shown in the application is sanitized and rendered in an isolated frame.

Platform hardening

- The API runs as a container built from a minimal official Python image. Build tools are removed from the final image.
- The database and the cache accept connections only from inside the hosting project.
- Unauthenticated endpoints are rate-limited. Personal access tokens are rate-limited per token.
- The API's public documentation exposes only the public API. Internal and administrative routes are not listed.
- The hosting provider restarts a failed container automatically and applies operating system and runtime patches to the managed services.

Vulnerability reports

Reports of a vulnerability are accepted at hi+support@lendpathway.com (Section 14).

11 Logging, monitoring, and audit records

Application logs

Every API process writes structured logs in one format: timestamp, level, process, logger, and message. Every request is logged with its method, path, status code, and duration. Tokens that appear in a path are replaced before logging. Document content, parsed values, and message bodies are not written to logs. Logs are held by the hosting provider and are reviewed during investigations.

Audit records in the application

RECORD	WHAT IT SHOWS
Usage ledger	One row for every billable action: parse, chat turn, web research, import, or verification. Each row names the organization, the Book, the job or chat, the provider, the model, and the cost. Rows are written in the same transaction as the work and are not editable through the application.
Parse jobs	A durable record of every parse: who or what started it, when, its status, its progress messages, and its outcome.
Document records	Who uploaded each document and when. Deletion is recorded, not erased.
Email intake records	Every message that was considered, its sender attribution, and what happened to it.
Sent emails	Every recipient of every email sent from the platform, with the delivery result.
Membership and tokens	Memberships, roles, invitations, and tokens with their creation and revocation times.

Monitoring

- The hosting provider monitors service health and restarts failed containers. The API exposes a health endpoint used for deploy checks.
- A background sweep runs every minute. It detects work that was interrupted by a restart, records it as failed, and delivers any pending notifications. Interrupted work is never left silent.
- Parse quality is monitored by the twice-daily regression run. Regressions are reported to the engineering team.
- Product analytics record feature usage for planning. They do not receive Customer Data.

12 Data retention, deletion, and export

The customer owns its data. Pathway keeps Customer Data for as long as the account is active and only as long as needed to provide the service.

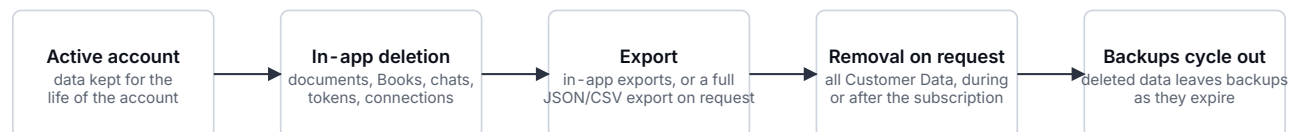


Figure 3. The data lifecycle.

Retention

DATA	RETENTION
Documents and parsed data	Life of the account. Removed on written request.
Connector grants and tokens	Deleted at once when the customer disconnects the service.

DATA	RETENTION
Chat history and sandbox	Sandbox files are discarded when the sandbox stops. History is kept until the chat is deleted.
Email intake	Message bodies are not stored. Attachments become documents. Intake records follow the account.
Usage and billing records	Life of the account, then as required for financial and legal records.
Backups	Deleted data persists in backups until the backup retention period ends, then is gone.
Logs	Short-term, per the hosting provider's retention.

Deletion

- **In the application.** Users delete documents, Books, chats, tokens, and connections at any time. A deleted item is removed from every view and every API response at once.
- **On request.** A customer can request removal of specific data or of all Customer Data, during the subscription or after cancellation, by writing to hi+support@lendpathway.com.
- **Legal holds.** Pathway retains data beyond these periods only where the law requires it.

Export

Users export spreadsheets, CSV files, and PDFs from the application at any time. A customer can also request a full export of its Customer Data in machine-readable formats such as JSON and CSV.

13 Availability, backup, and business continuity

Availability

- The web application is served from a global content delivery network with no single server.
- The API runs several worker processes in a managed container platform that restarts failed instances. Deploys do not interrupt service.
- The service degrades safely. If an AI provider or a connected service is unavailable, the affected action fails with a message and can be retried. Other functions continue.
- Long-running work such as parsing is recorded durably. A restart marks interrupted work as failed with a reason. It is not lost silently.

Backup and recovery

- The database is backed up automatically with point-in-time recovery.
- Object storage is designed for 99.999999999% durability. Objects are stored redundantly across multiple facilities within the region.
- The source code, the deployment configuration, and the database schema are version-controlled. A full environment can be recreated from the repository and the provider consoles.

Continuity

The platform is built on standard, replaceable dependencies. Self-hosted deployment and source code escrow are available under a separate agreement.

14 Incident response and vulnerability management

Incident response

A security incident is any event that compromises, or could compromise, the confidentiality, integrity, or availability of Customer Data or the platform. Pathway's engineering team owns incident response. The team follows these steps:

- 01 **Detect and triage.** Alerts, log review, a customer report, or a provider notice identify a possible event. An engineer confirms whether it is an incident and classifies its severity.
- 02 **Contain.** Stop the exposure: revoke credentials, rotate secrets, disable the affected path, or isolate the affected component.
- 03 **Assess.** Determine the scope: which organizations, which data, and which period.
- 04 **Notify.** Inform the administrators of affected organizations by email: what happened, which data was involved, and what is being done.
- 05 **Remediate.** Fix the cause, restore service, and verify that the exposure is closed.
- 06 **Review.** Write a post-incident report with the timeline, the cause, and the changes made.

Reporting a vulnerability

Send security reports to hi+support@lendpathway.com. Include steps to reproduce the issue. Do not access other customers' data.

15 Personnel and internal access

Pathway is operated by a small engineering team. Access to production is limited to the three founders. No contractor, vendor, or other employee has access to production systems or Customer Data.

CONTROL	PRACTICE
Who has access	Three named individuals. Each uses an individual account. There are no shared accounts.
Configuration changes	One designated administrator makes changes to production configuration, secrets, and infrastructure. The other two have access for operations and support.
Multi-factor authentication	Required on every account that can reach production: hosting, cloud storage, identity provider, source control, email, and domain registration.

CONTROL	PRACTICE
Purpose limitation	Staff access Customer Data only to operate the service, respond to a support request from the customer, investigate a security event, or comply with law.
Training	Every person with production access is trained on Pathway's security and data-handling policies.
Offboarding	If a person with access leaves, their accounts are removed and the secrets they could reach are rotated.
Confidentiality	Every person with access is bound by confidentiality obligations that cover Customer Data.

16 Subprocessors and connected services

A subprocessor is a provider that processes Customer Data on Pathway's behalf under Pathway's contract.

PROVIDER	SERVICE	DATA PROCESSED	LOCATION	WHEN
Amazon Web Services	Object storage (S3)	Customer documents, exports, chat files.	United States	Always
Railway	API compute, PostgreSQL, Redis	All application data.	United States	Always
Netlify	Web application hosting	Static files. Browser traffic to the application. No Customer Data at rest.	United States, global CDN	Always
Auth0 (Okta)	Identity provider	Name, email, phone, profile picture, login records, password hashes.	United States	Always
Google	Gemini API	Document content and extracted data for parsing; chat conversations and attachments.	United States	Parsing, chat
OpenAI	API	Document content for extraction when selected by the organization; business names for web research.	United States	Parsing, research
Vercel	Sandbox compute	Books and files the user attaches to a chat; a read-only API token.	United States	Chat
Baselayer	Business verification	Business name, address, tax identifier, owner names.	United States	On user request

PROVIDER	SERVICE	DATA PROCESSED	LOCATION	WHEN
Stripe	Billing	Billing contact, subscription, and payment details (held by Stripe only).	United States	Billing
Google Workspace	Transactional email, intake mailbox	Sign-in codes, invitations, intake messages and their attachments, replies.	United States	Always
Twilio (via Auth0)	SMS verification	Phone number and verification code.	United States	Phone sign-up only
PostHog	Product analytics	Event names, user and organization identifiers, pages viewed. No Customer Data.	United States	Always
fal.ai	Image generation	The text prompt only.	United States	Chat image generation
Microsoft	Office Online viewer	A time-limited URL to one spreadsheet or Word file, when a user opens a preview in the browser.	Global	On user action
Cloudflare	DNS	No Customer Data.	Global	Always

Customer - connected services

The following services are not subprocessors. The customer connects them, the customer's own agreement with the provider governs them, and the customer can disconnect them at any time. Pathway sends data to them only when the customer's users or the customer's configured automation ask it to.

SERVICE	GRANT	WHAT PATHWAY DOES WITH IT
Gmail	Per user, OAuth 2.0	Read the inbox, download attachments, send emails the user composes. Scopes: read-only mail, send mail, email address.
Google Drive	Per user, OAuth 2.0	Create and update the files Pathway exports. Scope limited to files Pathway creates.
Salesforce	Per organization, OAuth 2.0	Import opportunities and their files; write computed metrics back to the opportunity.
LendSaaS	Per organization, API key	Import leads, create deals, push worksheets and screening results.
OrgMeter	Per organization, API key	Push leads.

SERVICE	GRANT	WHAT PATHWAY DOES WITH IT
Slack	Per organization, incoming webhook	Post messages to the channels the customer selects.
Ramp	Per organization, partner program	Create merchant referrals from a Book and read the application status.

17 Privacy and compliance

Data use

TOPIC	DETAIL
Ownership	The customer retains all right, title, and interest in Customer Data.
Purpose limitation	Pathway uses Customer Data only to provide and maintain the service, respond to support requests, and comply with law.
No sale, no advertising	Pathway does not sell personal information and does not share it for cross-context behavioral advertising. Pathway uses no advertising trackers.
No deal interference	Pathway does not use Customer Data to solicit, broker, or interfere with the customer's financing transactions, customers, or business opportunities.
No model training	Pathway does not use Customer Data to train AI models. Its AI providers do not train on API data.
Aggregated data	Pathway may use aggregated or de-identified data that does not identify a customer or an individual for product improvement and industry analytics.
Google user data	Pathway's use of data from Google APIs follows the Google API Services User Data Policy, including the Limited Use requirements.
Individual rights	Pathway responds to requests to access, correct, delete, or export personal data within 30 days, or sooner where the law requires.
Regulations	Pathway complies with applicable data protection law, including the California Consumer Privacy Act and the General Data Protection Regulation where they apply.
Children	The platform is for businesses and is not directed at individuals under 16.

Certifications and attestations

Pathway does not hold an independent certification such as SOC 2 at this time. Pathway's security program is built on the controls described in this document and on the independently audited programs of its providers. Amazon Web Services, Railway, Netlify, Auth0, Google, OpenAI, Vercel, Stripe, and PostHog each publish a SOC 2 Type II report or an equivalent attestation through their trust pages. These reports are available from each provider's trust page.

Agreements

Use of the platform is governed by the Terms of Service at lendpathway.com/terms and the Privacy Policy at lendpathway.com/privacy, or by a signed customer agreement.

18 Shared responsibility

Pathway secures the platform. The customer secures its use of the platform. The table shows who is responsible for each area.

AREA	PATHWAY	CUSTOMER
Infrastructure	Selects and configures providers. Encrypts data in transit and at rest. Keeps the platform patched.	—
Application security	Authentication, authorization, tenant isolation, input validation, secure development.	Reports suspected issues.
User accounts	Provides sign-in methods, MFA, roles, and invitation controls.	Invites only authorized people. Assigns the least role needed. Removes people who leave. Enforces MFA in its identity provider.
API tokens	Hashes tokens, offers read-only tokens, allows revocation, rate-limits.	Stores tokens securely. Uses read-only tokens where possible. Revokes unused tokens.
Embedded views	Scopes each token to one Book. Expires tokens.	Shares embed links only with intended recipients.
Connected services	Stores grants securely. Uses the minimum scopes. Deletes grants on disconnect.	Decides which services to connect. Reviews who connected which inbox. Disconnects services no longer needed.
Email intake	Provides allow-lists and attribution. Processes only mail sent to the organization's address or inbox.	Configures allow-lists. Chooses which inbox is connected.
Chat agent	Limits the agent to read-only access and approval-gated sending.	Enables only the connectors a task needs. Reviews outputs before acting on them.
Customer Data content	Protects what is uploaded.	Has the right to upload the documents it uploads. Deletes data it no longer needs.
Downstream sharing	Logs every email sent and every push to a connected system.	Decides what to send to funders, partners, and CRMs.

AREA	PATHWAY	CUSTOMER
Incident response	Detects, contains, notifies affected customers, remediates.	Keeps administrator contact details current. Reports suspected incidents.

19 Answers to common questionnaire items

Where is our data stored?

In the United States. Documents are in a private Amazon S3 bucket. Application data is in a managed PostgreSQL database. Identity data is at Auth0.

Is our data encrypted?

Yes. TLS 1.2 or later in transit on every connection. Provider-managed encryption at rest for object storage, the database, and the cache. Selected credentials are also encrypted at the application layer.

Can other customers see our data?

No. Every record belongs to one organization. The API applies the caller's organization to every query.

Do you use our data to train AI?

No. Pathway does not train models. Its AI providers process requests under API terms that exclude training. OpenAI requests are sent with storage disabled.

Which AI providers see our documents?

Google (Gemini API) by default. OpenAI (API) when the organization selects it for extraction, and for web research of the business name. See Section 9.

Do you support single sign-on?

Yes. Google and Microsoft Entra ID through OpenID Connect. Your identity provider's MFA and conditional access policies apply to those sign-ins.

Do you support multi-factor authentication?

Yes, through Auth0, and through your own identity provider when you sign in with Google or Microsoft.

What roles exist?

Admin, member, and guest (read-only). API tokens can be issued as read-only. Embed tokens are read-only and limited to one Book.

How long are sessions?

Access tokens last 24 hours. Refresh tokens rotate, last at most 30 days, and expire after 15 days without use.

Who at Pathway can access our data?

Three named individuals, the founders, with MFA on every account. They access Customer Data only to operate the service, answer your support request, investigate a security event, or comply with law.

Can we delete our data?

Yes. Delete items in the application at any time, or request removal of specific data or all data.

Can we export our data?

Yes. Spreadsheets, CSV files, and PDFs export from the application at any time. A full export in JSON and CSV is available on request.

Are backups taken?

Yes. The database is backed up automatically with point-in-time recovery. Object storage is designed for eleven nines of durability.

Will you notify us of a breach?

Yes. Pathway emails the administrators of affected organizations with what happened, which data was involved, and what is being done.

Do you have a SOC 2 report?

Not at this time. Pathway's providers hold SOC 2 Type II reports. Pathway's own controls are described in this document.

Has the platform been penetration tested?

Pathway maintains automated authorization tests that run against a live API and database.

Do you have a vulnerability disclosure process?

Yes. Reports go to hi+support@lendpathway.com. See Section 14.

Can we run Pathway in our own environment?

Yes. A self-hosted deployment is available under a separate agreement, with optional source code escrow.

Do you process payment card data?

No. Payments are handled by Stripe's hosted checkout and billing portal. Card data never reaches Pathway.

20 Contact

Contact

Security, privacy, export, and deletion	hi+support@lendpathway.com
Legal entity	Pathway Systems LLC, doing business as LendPathway
Website	lendpathway.com
Terms of Service	lendpathway.com/terms
Privacy Policy	lendpathway.com/privacy